Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] What is claimed is:

1. A method for determining whether a communication device is permitted to access communication service in a communication network, the communication device comprising:
a data memory capable of storing ciphertext access information; and
an inerasable memory capable of storing a deciphering key in a non-volatile way;
the method comprising:
reading the deciphering key in the inerasable memory and the ciphertext access information in the data memory; and
deciphering the ciphertext access information to plaintext access information according to the deciphering key by using a predetermined cryptography algorithm, and determining whether the communication device is permitted to access communication service in the communication network accordingly.

[c2] 2. The method of claim 1 wherein the cryptography algorithm is an asymmetric encryption-and-decryption al-

gorithm.

[c3] 3. The method of claim 1 wherein the data memory is a non-volatile memory.

[c4] 4. The method of claim 1 further comprising:
enciphering access information corresponding to the communication device into the ciphertext access information by the cryptography algorithm according to an enciphering key, wherein the enciphering key corresponds to the deciphering key; and
recording the ciphertext access information in the data memory.

[c5] 5. The method of claim 4 further comprising:
generating the enciphering key and the corresponding deciphering key according to the cryptography algorithm before generating the ciphertext access information according to the enciphering key.

[c6] 6. The method of claim 4, wherein the communication network comprises a service provider capable of providing communication service to the communication device; there being a database in the service provider for recording the enciphering key and the access information corresponding to the communication device.

[c7] 7. The method of claim 6, wherein when generating the

ciphertext access information according to the enciphering key, the service provider enciphers the access information corresponding to the communication device to generate the ciphertext access information according to the enciphering key stored in the database.

[c8] 8. The method of claim 7, wherein when recording the ciphertext access information in the data memory, transmitting the ciphertext access information from the service provider to the communication device via the communication network, and recording the ciphertext access information in the data memory with the communication device.

[c9] 9. The method of claim 4, wherein the enciphering key is different from the deciphering key.

[c10] 10. The method of claim 1, wherein when determining whether the communication device is permitted to access communication service of the communication network according to the plaintext access information, determining whether the plaintext access information conforms to predetermined access information; the communication device being determined permitted to access the communication service of the communication network if the plaintext access information conforms to the predetermined access information.

[c11] 11. The method of claim 1 in which the communication device further comprises a subscriber identification module card (SIM card) capable of recording a subscriber identification number, and a predetermined identification number is recorded in the plaintext access information, wherein when determining whether the communication device is permitted to access communication service in the communication network according to the plaintext access information, determining whether the subscriber identification code conforms to the predetermined identification code; the communication device being permitted to access the communication service if the predetermined identification code and the subscriber identification code correspond to each other, and the communication device being not permitted to access the communication service and having access to the communication network stopped if the predetermined identification code and the subscriber identification code do not correspond to each other.

[c12] 12. A communication device utilized in a communication network for accessing communication service of the communication network; the communication device comprising:

a data memory capable of storing ciphertext access information in a non-volatile way;

an inerasable memory capable of storing a deciphering key in a non-volatile way; and

a processor capable of controlling operation of the communication device;

wherein before the communication device accesses the communication service of the communication network, the processor reads the deciphering key in the inerasable memory and the ciphertext access information in the data memory, utilizes a predetermined cryptography algorithm to decipher the ciphertext access information to plaintext access information according to the deciphering key, and determines whether the communication device is permitted to access communication service of the communication network according to plaintext access information.

[c13] 13. The communication device of claim 12 wherein the cryptography algorithm is an asymmetric encryption-and-decryption algorithm.

[c14] 14. The communication device of claim 12 in which the communication network comprises a service provider for providing communication service to the communication device; there being a database in the service provider capable of recording the enciphering key and the access information corresponding to the communication device; the ciphertext access information being generated by

enciphering the access information corresponding to the communication device by the cryptography algorithm according to the enciphering key, wherein the enciphering key corresponds to the deciphering key.

[c15] 15. The communication device of claim 14 wherein the enciphering key and the corresponding deciphering key are generated according to the cryptography algorithm.

[c16] 16. The communication device of claim 14 wherein the ciphertext access information is transmitted from the service provider to the communication device via the communication network, and recorded in the data memory by the communication device.

[c17] 17. The communication device of claim 12 wherein when the processor determines whether the communication device is permitted to access communication service according to the plaintext access information, the processor determines whether the plaintext access information conforms to predetermined access information; wherein the processor determining the communication device is permitted to access the communication service if the plaintext access information conforms to the predetermined access information.

[c18] 18. The communication device of claim 12 in which the

communication device further comprises a SIM card capable of recording a subscriber identification number, and a predetermined identification code is recorded in the plaintext access information, wherein when the processor determines whether the communication device is permitted to access communication service according to the plaintext access information, the processor determines whether the subscriber identification code conforms to the predetermined identification code; the communication device being permitted to access the communication service if the predetermined identification code and the subscriber identification code correspond to each other, and the communication device being not permitted to access the communication service and access to the communication network being stopped if the predetermined identification code and the subscriber identification code do not correspond to each other.

[c19] 19. The communication device of claim 12 in which the communication device is a cell phone, and the communication network is a wireless communication network.

[c20] 20. A method applied in a communication network, wherein the communication network comprises a plurality of communication devices and each communication device comprises an inerasable memory and a data

memory; the method being capable of determining whether each communication device is permitted to access communication service of the communication network; the method comprising:

providing a plurality of different enciphering keys and a plurality of deciphering keys according to a cryptography algorithm, wherein each enciphering key corresponds to each deciphering key;

providing different corresponding enciphering keys to different communication devices;

enciphering access information corresponding to each communication device to ciphertext access information by the cryptography algorithm according to the enciphering key corresponding to the communication device;

storing deciphering keys corresponding to the enciphering keys corresponding to each of the communication devices in the inerasable memory;

storing ciphertext access information of each communication device in the data memory of the communication device; and

when determining whether a communication device is permitted to access the communication service, deciphering the ciphertext access information in the data memory by the cryptography algorithm according to the enciphering key stored in the inerasable memory, and determining whether the communication device is per-

mitted to access the communication service according to the deciphered ciphertext access information.

[c21] 21. The method of claim 20, wherein the deciphering keys corresponding to different enciphering keys are different.

[c22] 22. The method of claim 20, wherein the cryptography algorithm is an asymmetric encryption-and-decryption algorithm such that an enciphering key is not equal to the corresponding deciphering key, and when a plaintext is enciphered into a ciphertext according to the enciphering key by the cryptography algorithm, the cryptography algorithm cannot decipher the ciphertext into the original plaintext according to the enciphering key.

[c23] 23. The method of claim 20, wherein the communication network further comprises a service provider capable of transmitting signals and providing communication service among communication devices; there being a database in the service provider, and the method further comprising storing enciphering keys corresponding to each communication device in the database.

[c24] 24. The method of claim 20 in which the communication device is a cell phone, and the communication network is a wireless communication network.